NUI Galway
OÉ Gaillimh

Semester II Examinations, 2021/2022

Exam Code(s)	4BCT1, 1MECE1, 1OA1, 1EM1
Exam(s)	Year 4 BSC in Computing Science and Information Technology, Masters in Electronic and Computer Engineering
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	Special Paper
External Examiner(s)	Dr. Ramona Trestian
Internal Examiner(s)	Professor Michael Madden
	*Dr. Michael Schukat

Instructions: Time allowed: **2** hours
Answer any 3 questions. All questions carry equal marks.

Duration	2 hrs
No. of Answer books	2
Requirements:	
Handout	
MCQ	
Statistical Tables	
Graph Paper	
Log Graph Paper	
Graphic Material in colour	YES
No. of Pages	5
Discipline(s)	Information Technology

Q.1.

(i) Consider NUI Galway computer services decide to setup an IPsec-based VPN (encryption only) to St. Angela's College in Co. Sligo. Additional authentication and / or encryption between endpoints may be added on demand, subject to the University's security policy. Explain in some detail, how IPsec accommodates all these requirements. In your answer, make reference to the following:

- Transport mode versus tunnel mode connections
- ESP and AH, and their respective protocol headers
- Anti-replay window
- Combined SA, with particular focus on end-to-end authentication and encryption.

[8 marks]

(ii) Distinguish between the following port scan types:

- Network ping sweeps
- TCP connect scan
- TCP SYN scan
- TCP FIN scan
- UDP scan

Using an example explain how port knocking can deter some port scans.

[5 marks]

(iii) Explain the functionality of S-boxes and P-boxes. Use diagrams to support your answer.

[2 marks]

(iv) Using an example explain how a simple substitution cipher can be broken via a letter frequency distribution analysis.

[2 marks]

PTO

Q.2.

(i) HomeAuto® is a start-up company for home automation / IoT products. Their flagship home area network product is based on a Wi-Fi access point that communicates with and manages a variety of wireless sensors and actuators, e.g. thermostats and motion detectors. In order to avoid 3rd party products to be used, and to provide secure end-to-end communication, the company decides to install digital certificates on every device. Explain, how such a solution would work. In your answer, make reference to:

- X.509 certificates and a suitable certificate structure for the company's devices
- The purpose of the CA and a suitable CA hierarchy
- How certificate revocation could be implemented
- How certificate extensions could be used
- How the device validation and key generation for secure device-to-access point communication would work.

[8 marks]

(ii) Distinguish between the following **GDPR principles**

- Lawfulness, fairness and transparency
- Data minimisation
- Storage limitation
- Integrity and confidentiality (security)

Use examples to support your answer.

[2 marks]

(iii) Design a stream cipher that is based on two combined 12-bit LFSRs of your choice. Using an example show how the algorithm works and how a serial bitstream can be encoded and decoded.

[5 marks]

(iv) Using a diagram show how a private key block cipher (like DES) can be used to calculate a message authentication code (MAC) over a given input.

[2 marks]

PTO

Q.3.

(i) Outline the various steps involved to provide end-point authentication in a computer network using

- Private key encryption
- Public key encryption
- Zero-knowledge protocols

thereby outlining advantages and disadvantages of each approach.

[8 marks]

(ii) Modern block ciphers support various modes of operation, including:
- Electronic codebook (ECB) mode
- Cipher block chaining (CBC) mode

Distinguish between these two modes and summarise their advantages and disadvantages.

[2 marks]

(iii) Hash chains and rainbow tables are used to recover hashed passwords. Outline similarities and differences between both concepts and give a comprehensive example of how a hashed password can be recovered by a rainbow table.

[5 marks]

(iv) Using an example show how a Rotor Cipher consisting of 3 rotors works.

[2 marks]

PTO

Q.4.

(i) Consider you are asked to provide a security protocol for a wireless sensor network based on WEP (for encryption / authentication) and Diffie-Hellman (for peer-to-peer key negotiation). Using diagrams and examples to support your answer outline how such a system would work, thereby highlighting limitations and weaknesses.

[8 marks]

(ii) Explain in some detail the purpose, structure and inner workings of a Feistel cipher and a Feistel network.

[3 marks]

(iii) Discuss the three security properties that are associated with cryptographic hash functions. Use examples to explain why they are needed.

[4 marks]

(iv) Outline four methods that can be used to render rainbow tables useless for password recovery.

[2 marks]